REMARKS

As previously stated in this amendment, amendments to the drawings have been made prior to the formal set of drawings being filed with the Patent and Trademark Office. The set of formal drawings that was submitted with the Notice to File Corrected Application Papers on July 27, 2001, (and received by the PTO on July 30, 2001) is correct and contains all of the drawing changes made to the informal set of drawings (which were filed with the application on December 19, 2000). The updates included in the formal set of drawings filed are listed below :

In Figure 8, second row, PE_3 (X-Phase), reference numeral 20 was incorrect and has been updated to 200; in Figure 14, Register BN reference numeral 272 has been updated to 298 in two occurrences; and in Figure 16, the last number in the column on the right-hand bottom side has been updated to 24, not 34, as originally depicted in the informal set of drawings filed with the patent application. Please note that Figure 13 has been split by the draftsperson into Figures 13A and 13B, respectively. In the specification, where Figure 13 is mentioned, it is to be considered as encompassing both Figures 13A and 13B inclusively.

At present, applicants' Claim 3 stands rejected under 35 U.S.C. § 101. Applicants' Claims 1, 2, 4, 5 and 6 stand rejected under 35 U.S.C. § 112, first paragraph. These claims also stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1 and 2 stand rejected under 35 U.S.C. § 102(b) based upon the article by Tenca and Koc (referred to hereinafter as Tenca). Claim 3 stands rejected under 35 U.S.C. § 102(a) based upon the cited article by Compaq Computer Corporation titled "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment." Claims 4-6 stand rejected under 35 U.S.C. § 103(a) based upon the aforementioned article by the Compaq Computer Corporation in view of the

article by Tenca. In light of the amendments made herein and the comments presented below all, of these rejections are respectfully traversed. Accordingly, Claims 1-6 remain pending in the present application.

The aforementioned rejections are considered below in the order in which the Examiner has presented them in the Office Action.

Accordingly, attention is first directed to the rejection of applicants' claim 3 under 35 U.S.C. § 101. In this regard, it is noted that applicants have clarified the recited digital processing method originally stated in Claim 3 by further indicating that this method uses a calculating engine which performs operations modulo an integer. It is not now nor was it ever applicants' intent to claim a processing method that did not employ some form of photonic or electronic circuitry. Accordingly, it is seen that the claimed method is not directed to an abstract idea and that it is in fact tied to the technological arts of digital computing. It is further clear that the result that is produced, namely A^B is an extremely useful result in encrypting and decrypting communications and data. The rejection of claim 3 under 35 U.S.C. § 102 is considered below. However, with respect to the rejection under 35 U.S.C. § 101, it is noted that the Examiner has correctly anticipated that applicants will and have changed Claim 3 so as to be in total compliance with 35 U.S.C. § 101. Accordingly, it is therefore respectfully requested that the rejection of Claim 3 under 35 U.S.C. § 101 be withdrawn.

Attention is next directed to the rejection of Claims 1, 2, 4, 5 and 6 under 35 U.S.C. § 112, first paragraph. In this regard, it is noted that applicants have amended all of the subject claims to include the omitted numeral "2." This was a typographical error and does not in any way or sense rise to the level of a rejection under 35 U.S.C. § 112. There is no question whatsoever as to whether or not the intended claims comply with the written description. This is a simple typographical error and nothing more. There is no issue as to whether or not the applicants had possession of the invention.

Accordingly, since this typographical error has been corrected, as of right, by the present response, it is seen that the rejection of Claims 1, 2, 4, 5 and 6 under the first paragraph of 35 U.S.C. § 112 cannot be sustained. Accordingly, it is respectfully requested that it too be withdrawn.

The Examiner has also rejected applicants' Claims 1, 2, 4, 5 and 6 under the second paragraph of 35 U.S.C. § 112. Again, it is pointed out that this rejection is solely based upon a simple typographical error, nothing more. Nonetheless, applicants' attorney does express his appreciation to the Examiner for pointing out this error. As with the rejection of Claims 1, 2, 4, 5 and 6 under the first paragraph of 35 U.S.C. § 112, this rejection also under the second paragraph is likewise no longer sustainable as a result of the corrections made herein. Accordingly, it is therefore also respectfully requested that the rejection of Claims 1, 2, 4, 5 and 6 under the second paragraph of 35 U.S.C. § 112 also be withdrawn.

Attention is next directed to the rejection of Claims 1 and 2 under 35 U.S.C. § 102 based upon the aforementioned article by Tenca titled "A Scalable Architecture for Montgomery Multiplication." In this regard, it is first noted that the article by Tenca is directed to multiplication operations. In contrast, it is seen that applicants' Claims 1 and 2 are directed to methods for determining A mod N. Nowhere in either of these claims is Montgomery Multiplication mentioned. Furthermore, and more importantly, it is noted that applicants' claims are directed to the processing of multi-bit word segments. In short, in applicants' claimed process, the input A is represented in the form $A_i 2^{mk} + A_0$. In short, in applicants' claimed process, the "chunks" of information processed by the calculating engine is k bits each. In particular, the variable A is broken up into m words each having k bits. In contrast, this blocking of the variables processed by a Montgomery Multiplier is not present in the article by Tenca. In point of fact, this form of processing is specifically taught against. In particular, the Examiner's attention is

directed to the following two quotations from section 4 starting on page 97 of the paper by Tenca:

> "Therefore, an algorithm which performs bit-level computations and produces word-level outputs would be the best choice . . . ."
>
> "We propose an algorithm in which the operand *Y* (multiplicand) is scanned word-by-word, and the operand *X* (multiplier) is scanned bit-by-bit."

One of the principle concerns expressed in the article by Tenca is scalability. Accordingly, the teachings of Tenca require that one of the operands be treated in a bit-by-bit fashion. This can be seen from the quotation from Tenca found on page 98 which states:

> "Once the precision is exhausted, another bit of *X* is taken, and the scan is repeated . . . What varies is the number of loop iterations required to accomplish the modular multiplication."

Accordingly, the teachings of Tenca are in direct opposition to the treatment of a variable such as *A* in applicants' claimed process and apparatus into blocks of *m* chunks of *k* bits each.

As a matter of clarification, it is noted that in applicants' claimed specification *k* is the size of the words processed by the calculating engine in bits. In contrast, in Tenca the term "word" refers to the entire variable *A* not to *k* bit chunks which are processable by a calculating engine.

Accordingly, it is seen that applicants' Claims 1 and 2 are in no way anticipated by the teachings of Tenca. In point of fact, the teachings of Tenca are actually contrary to those found in applicants' specification and in Claims 1 and 2. Accordingly, it is

respectfully requested that the rejection of applicants' Claims 1 and 2 under 35 U.S.C. § 102 be withdrawn.

Attention is next directed to the rejection of applicants' Claim 3 under 35 U.S.C. § 102(a) based upon the Compaq article. In this regard, it is noted that applicants do not disagree with the Examiner's mapping of variables from the Compaq article to those found in applicants' Claim 3. However, the results returned by the computational flow diagram in Figure 1 from the Compaq article produce the following results when this mapping is carried out:

$$(((A_{pB} - (A_{qB} \bmod N_p))(N_q^{-1} \bmod N_p)) \bmod N_p)N_q + A_{qB}.$$

In contrast, it is seen in line 15 of applicants' Claim 3 that the result produced, namely A^B is as follows:

$$N_q((A_{pB} - A_{qB}) \bmod N_p)(N_q^{-1} \bmod N_p) \bmod Np + A_{qB}.$$

Accordingly, it is seen that, while similar, the results produced are not identical. However, rejection of claims under 35 U.S.C. § 102 requires identity. Accordingly, the rejection of Claim 3 under 35 U.S.C. § 102 is not sustainable. Thus, it is respectfully requested that this rejection be withdrawn.

Attention is next directed to the rejection of Claims 4, 5, and 6 under 35 U.S.C. § 103(a) based upon the article by Compaq in view of the article by Tenca. As above, it is again noted that all of the recited claims recite a processing method for an apparatus in which the variables being processed are considered in *m* blocks of *k* bits each. As seen in the discussion above, Tenca specifically teaches away from the utilization of block structures and instead requires the utilization of bit-by-bit processing in order to provide a degree of scalability. Accordingly, it is seen that the combined teachings fly in

the face of the recited claim language which clearly contemplates variables being present in the form of words having *m* blocks of *k* bits each. Neither the article by Tenca nor the article by Compaq teach, disclose or suggest this representational and computational modality. Accordingly, it is seen that those of ordinary skill in the art would not be led to processes or systems in which variable quantities are considered in *k* bit chunks. (Again, as above, it is noted that applicants reference to *k* bit words is not the same as the words referred to in the cited documents. Applicants' "words" are *k* bit chunks, while in contrast the cited articles refer to words as the entire representation for variables such as *A* and *B*.) Accordingly, since the partition processing in *k* bit chunks is specifically referred to in the rejected claims and since none of the art cited teaches, discloses or even suggests such a processing modality, it is clear that the rejection of applicants' Claims 4, 5 and 6 under 35 U.S.C. § 103 (a) cannot be sustained. Furthermore, it is noted that one of the cited articles, namely Tenca, specifically teaches against block processing. Accordingly, it is therefore respectfully requested that the rejection of applicants' Claims 4, 5 and 6 under 35 U.S.C. § 103 (a) be withdrawn.

It is noted that the present response does not require the payment of any additional fees. It is also noted that the amendments to applicants' claimed specification are being made herein as of right.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless applicants have argued herein that such amendment was made to distinguish over a particular cited document or combination of documents.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any other matters which the Examiner

feels could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

Aug. 26, 2004
Date

Lawrence D. Cutter
LAWRENCE D. CUTTER, Sr. Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com